

# VANISHING AND NON-VANISHING DIRICHLET TWISTS OF $L$ -FUNCTIONS OF ELLIPTIC CURVES

JACK FEARNLEY, HERSHY KISILEVSKY<sup>†</sup>, AND MASATO KUWATA

ABSTRACT. Let  $L(E/\mathbb{Q}, s)$  be the  $L$ -function of an elliptic curve  $E$  defined over the rational field  $\mathbb{Q}$ . We examine the vanishing and non-vanishing of the central values  $L(E, 1, \chi)$  of the twisted  $L$ -function as  $\chi$  ranges over Dirichlet characters of given order.

## 1. INTRODUCTION.

Let  $E/\mathbb{Q}$  be an elliptic curve defined over the field  $\mathbb{Q}$ . Denote by

$$L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n n^{-s}$$

its  $L$ -function.

By the proof [BCDT],[TW] of the modularity of elliptic curves over  $\mathbb{Q}$ , we know that  $L(E, s)$  has an analytic continuation for all  $s \in \mathbb{C}$ , and satisfies the functional equation

$$\Lambda(E, s) = w_E \Lambda(E, 2 - s),$$

where  $\Lambda(E, s) = (\sqrt{N_E}/2\pi)^s \Gamma(s) L(E, s)$ ,  $N_E$  is the conductor of  $E/\mathbb{Q}$ , and  $w_E = \pm 1$ .

For a primitive Dirichlet character  $\chi$  of conductor  $\mathfrak{f}_\chi$ , the *twist* of  $L(E/\mathbb{Q}, s)$  by  $\chi$  is

$$L(E, s, \chi) = \sum_{n \geq 1} \chi(n) a_n n^{-s}.$$

Then we also know that the  $L$ -function  $L(E, s, \chi)$  has an analytic continuation and if  $\mathfrak{f}_\chi$  is coprime to  $N_E$ , satisfies the functional equation

$$\Lambda(E, s, \chi) = w_E \chi(N_E) \tau(\chi)^2 \mathfrak{f}_\chi^{-1} \Lambda(E, 2 - s, \overline{\chi}),$$

---

<sup>†</sup>This work was supported in part by grants from NSERC and FCAR.

where  $\Lambda(E, s, \chi) = (\mathfrak{f}_\chi \sqrt{N_E}/2\pi)^s \Gamma(s) L(E, s, \chi)$  and  $\tau(\chi)$  is the Gauss sum

$$\tau(\chi) = \sum_{c=0}^{\mathfrak{f}_\chi-1} \chi(c) \exp(2\pi i c/\mathfrak{f}_\chi).$$

We consider the question of the vanishing or non-vanishing of  $L(E/\mathbb{Q}, s, \chi)$  at  $s = 1$  as  $\chi$  ranges over sets of Dirichlet characters of fixed order. For integers  $n \geq 1$ , let  $\mathcal{X}(n)$  denote the set of primitive Dirichlet characters of order exactly equal to  $n$ , i.e.

$$\mathcal{X}(n) = \{\chi \mid \chi^n = \chi_0 \text{ and } \chi^d \neq \chi_0 \text{ for } d < n\}.$$

where  $\chi_0$  is the principal character.

Given  $n$  a positive integer and  $X > 0$ , we consider

$$\mathfrak{F}_E(n, X) = \mathfrak{F}_E^1(n, X) = \#\{\chi \in \mathcal{X}(n) \mid \mathfrak{f}_\chi \leq X \text{ and } L(E, 1, \chi) = 0\},$$

or more generally

$$\mathfrak{F}_E^r(n, X) = \#\{\chi \in \mathcal{X}(n) \mid \mathfrak{f}_\chi \leq X \text{ and } \text{ord}_{s=1} L(E, s, \chi) \geq r\}.$$

These functions have been extensively studied in the case that  $n = 2$ , and there are many results and conjectures that describe  $\mathfrak{F}_E^r(2, X)$  as  $X \rightarrow \infty$ . Some of these will be reviewed in §2.

Given a Dirichlet character  $\chi$ , let  $K_\chi$  be the cyclic extension of  $\mathbb{Q}$  (of conductor  $\mathfrak{f}_\chi$ ) which corresponds to  $\chi$ . We write  $K_\chi = K$  when the character  $\chi$  is understood.

The Birch & Swinnerton-Dyer conjecture equates the order of vanishing of  $L(E/\mathbb{Q}, s)$  at  $s = 1$  to the  $\mathbb{Z}$ -rank of the Mordell-Weil group  $E(\mathbb{Q})$ . More generally (see [Roh]), the order of vanishing of  $L(E/\mathbb{Q}, s, \chi)$  at  $s = 1$  is conjectured to be the rank of the “ $\chi$ -component”  $E(K)^\chi$  of  $E(K)$ , where  $K = K_\chi$ . Here  $\text{rank}_{\mathbb{Z}} E(K)^\chi = \dim_{\mathbb{C}} (\mathbb{C} \otimes E(K))^\chi$  is the dimension of the  $\chi$  eigenspace of  $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$  as a  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -space.

The algebro-geometric version of vanishing (resp. non-vanishing) of  $L(E/\mathbb{Q}, 1, \chi)$  is whether the  $\chi$ -component  $E(K)^\chi$  of  $E(K)$  has positive rank (resp.  $\text{rank}_{\mathbb{Z}} E(K)^\chi = 0$ ) as  $K_\chi$  ranges over the corresponding cyclic extensions of  $\mathbb{Q}$ . This amounts to asking whether or not  $\text{rank}_{\mathbb{Z}} E(K_\chi) > \text{rank}_{\mathbb{Z}} E(F)$  for all proper subfields  $F \subset K_\chi$ .

We rely on Kato's important result generalizing Kolyavagin's theorem [Kol] which asserts that if the  $\chi$ -component of  $E(K_\chi)$  has positive rank, then  $L(E/\mathbb{Q}, 1, \chi) = 0$  (see Scholl [Sch].)

Suppose that  $\chi$  is a character of prime order  $\ell$ ,  $K = K_\chi$  is the field corresponding to  $\chi$ , and let  $V = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ . Then  $V$  is a representation space for  $G = \text{Gal}(K/\mathbb{Q})$  with  $\dim_{\mathbb{Q}} V = \text{rank}_{\mathbb{Z}} E(K)$ . Since  $G$  is a cyclic group of prime order, the  $\mathbb{Q}$ -irreducible characters of  $G$  are the trivial character  $\chi_0$  and an irreducible of degree  $\ell - 1$  containing all the conjugates of  $\chi$ . Hence if  $\text{rank}_{\mathbb{Z}} E(K) > \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$ , then the  $\chi^j$ -component of  $E(K)$  has positive rank for each  $j = 1, \dots, \ell - 1$ . It follows from Kato's theorem (Kolyavagin [Kol], if  $\ell = 2$ ) that if  $\text{rank}_{\mathbb{Z}} E(K)^\chi > 0$  for a non-trivial character of prime order  $\ell$ , that  $L(E/\mathbb{Q}, 1, \chi^j) = 0$  for each  $j = 1, \dots, \ell - 1$ . In this context, it will follow from a modular symbol computation in §3 that if  $L(E/\mathbb{Q}, 1, \chi) = 0$  for a single character of order  $\ell$  then  $L(E/\mathbb{Q}, 1, \chi^j) = 0$  for all  $j = 1, \dots, \ell - 1$ .

In this paper we consider the case  $\ell \geq 3$ . Our main Theorems (proved in §3, §5 and §6) are:

**Theorem A.** *If  $L(E/\mathbb{Q}, 1) \neq 0$ , then for all but a finite number of primes  $\ell$ , the number of non-vanishing twists by Dirichlet characters of order  $\ell$  and prime conductor satisfies*

$$\#\{\chi \in \mathcal{X}(\ell) \mid \mathfrak{f}_\chi = p \text{ prime} < X, L(E, 1, \chi) \neq 0\} \gg X/\log X.$$

**Theorem B.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ , and let  $L(E, s)$  be the associated  $L$ -function. If there is at least one character  $\chi_1 = \chi_0$ , or  $\chi_1 \in \mathcal{X}(3)$  such that  $E(K_{\chi_1})$  is infinite, then there are infinitely many cubic characters  $\chi \in \mathcal{X}(3)$  such that  $L(E, 1, \chi) = 0$ .*

**Theorem C.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with at least 6 rational points. Then there exist infinitely many  $\chi \in \mathcal{X}(3)$  such that the rank of the Mordell-Weil group  $\text{rank}_{\mathbb{Z}} E(K_\chi) > \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$ . As a consequence, there are infinitely many cubic characters  $\chi \in \mathcal{X}(3)$  such that  $L(E, 1, \chi) = 0$ .  $\square$*

A random matrix model for the distribution of zeros of  $L$ -functions in families was introduced by Katz and Sarnak ([KS]) and was related to the distribution of eigenvalues of random matrices taken from classical groups. They proved that

the model held in the case of  $L$ -functions attached to certain families of curves over finite fields. This heuristic was applied by Conrey, Keating, Rubinstein and Snaith ([CKRS]) to give rather precise predictions for the frequency of vanishing of the central values of quadratic twists of elliptic  $L$ -functions with sign  $+1$ . In [DFK1] and [DFK2], their work was adapted to predict the frequency of vanishing of  $L(E, 1, \chi)$  of twists of the  $L$ -function by Dirichlet characters  $\chi$  of fixed order greater than 2. The predictions for  $\mathfrak{F}_E(n, X)$  as  $X \rightarrow \infty$  become

$$\begin{aligned} \mathfrak{F}_E(n, X) &\sim b_E X^{1/2} \log^{a_E}(X) \quad \text{if } \phi(n) = 2 \\ &\sim \log^{a'_E}(X) \quad \text{if } \phi(n) = 4 \\ &\text{is bounded if } \phi(n) \geq 6 \end{aligned}$$

where  $\phi$  is Euler's totient and  $b_E, a_E, a'_E \neq 0$ . These predictions compare favourably to the numerical computations reported in [DFK1] and [DFK2].

In §7 we will work out the case of a curves with rational 3-torsion, and for many such curves  $E/\mathbb{Q}$  we will obtain the strong lower bounds

$$\mathfrak{F}_E(3, X) \gg X^{1/2}.$$

## 2. THE QUADRATIC CASE

If  $\chi$  is a *real* primitive character, i.e., if  $\chi^2 = \chi_0$ , then  $\chi = \chi_0$  or  $\chi = \left(\frac{\cdot}{D}\right)$  is the character of a quadratic field  $\mathbb{Q}(\sqrt{D})$ , and  $\mathfrak{f}_\chi = D$ , a fundamental discriminant. In the latter case,  $L(E, s, \chi)$  is the  $L$ -function of the elliptic curve  $E^D$ , the twist of  $E$  by  $D$ . Since  $\chi$  is real, the functional equation relates  $L(E, 1, \chi)$  to itself and necessarily vanishes if the sign of the functional equation  $w_{E^D} = -1$ . For a primitive quadratic character  $\chi$ , with  $(\mathfrak{f}_\chi, N_E) = 1$ , the sign of the functional equation for  $L(E, s, \chi)$  is equal to  $\chi(-N_E)$  times that of  $L(E, s)$ . Hence we see that  $L(E, 1, \chi) = 0$  for at least one half of such quadratic characters. It follows from the theorem of Waldspurger [Wal] (see also Ono-Skinner [OS]), that there are an infinite number of quadratic characters  $\chi$  for which  $L(E, 1, \chi) \neq 0$ .

Gouvêa-Mazur [GM] show, assuming the parity conjecture (that  $\text{rank}_{\mathbb{Z}} E(\mathbb{Q})$  of an elliptic curve,  $E$ , has the same parity as  $\text{ord}_{s=1} L(E, s)$ ), that there are infinitely many twists  $D$  with Mordell-Weil groups of rank at least 2. They show (under the

parity conjecture) that

$$\mathfrak{F}_E^2(2, X) = \#\{\chi \in \mathcal{X}(2) \mid \mathfrak{f}_\chi < X, L(E, 1, \chi) = 0 = L'(E, 1, \chi)\} \gg X^{1/2-\epsilon}.$$

Stewart-Top [ST] have removed the parity conjecture in the Gouvêa-Mazur result and obtain  $X^{1/7-\epsilon}$  ( $X^{1/6-\epsilon}$  for some special families of curves). Liem Mai [Mai] proved that the number of cubic twists of  $x^3 + y^3 = d$  for which the corresponding  $L$ -function has at least a double zero at  $s = 1$  is  $\gg X^{2/3-\epsilon}$ , also assuming the parity conjecture. Goldfeld, [Gol], conjectured that for a given elliptic curve  $E$  defined over  $\mathbb{Q}$ , asymptotically one half of the quadratic twists  $L(E, s, \chi)$  of  $L(E, s)$  will have a *simple* zero at  $s = 1$  and that asymptotically one half will be non-vanishing.

Murty-Murty [MM] and Bump-Friedberg-Hoffstein [BFH] have shown that

$$L(E, 1, \chi) = 0 \neq L'(E, 1, \chi)$$

occurs for infinitely many quadratic characters  $\chi$ .

In the case of twists of  $L(E, s)$  by characters of higher order, i.e., by characters  $\chi$  of order  $\ell \geq 3$ ,  $\chi$  assumes complex values and the functional equation relates  $L(E, s, \chi)$  to  $L(E, s, \overline{\chi})$ . Consequently, there is no longer a “forced” central zero due to the sign of the functional equation. It is an interesting question to determine the number of characters  $\chi$  in a given set of characters  $\mathcal{X}$  for which  $L(E, 1, \chi) = 0$ .

Rohrlich [Roh2] has shown that among all Dirichlet characters  $\chi$  with conductors supported on a finite set of primes, only finitely many can vanish at  $s = 1$ . Stefanicki [Ste], Akbary [Akb], and Murty [Mur] give various nonvanishing results for twisted central  $L$ -values and of particular interest is the result of Chinta [Chi], which states that for sufficiently large prime  $q$

$$\#\{\chi \mid \mathfrak{f}_\chi = q, L(E, 1, \chi) = 0\} \ll q^{7/8+\epsilon}.$$

### 3. NON-VANISHING OF TWISTS OF PRIME ORDER

Let  $\ell > 2$  denote an *odd prime* number and suppose that  $E$  is an elliptic curve defined over the rational field  $\mathbb{Q}$ . Let  $\chi \in \mathcal{X}(\ell)$  be a Dirichlet character. We will demonstrate a congruence between the algebraic part of  $L(E, 1)$  and the algebraic part  $L(E, 1, \chi)$ . In the case that  $L(E, 1) \neq 0$  this will allow us to prove that for all but a finite number of primes  $\ell$ , there are infinitely many characters  $\chi \in \mathcal{X}(\ell)$  such that  $L(E, 1, \chi) \neq 0$ .

Let  $f$  be the weight two modular form of level  $N$ . We recall the properties of modular symbols following Mazur, Tate and Teitelbaum ([MTT]).

For  $\alpha$  and  $\beta$  in the upper half plane, define a modular symbol  $\{\alpha, \beta\}$  as a linear functional on cuspforms  $f \in S_2(N)(= S_2(\Gamma_0(N)))$  by

$$\{\alpha, \beta\}f = \frac{1}{2\pi i} \int_{\alpha}^{\beta} f(z)dz.$$

For a fixed cuspform  $f \in S_2(N)$ , we will write  $\{\alpha, \beta\}$  for  $\{\alpha, \beta\}f$ . The properties of the modular symbol which are important for our purposes are summarized below:

**Proposition 3.1** (*L-function relation*). *The L-series of a cuspform at its critical point can be expressed as a modular symbol*

$$L(f, 1) = \{\infty, 0\}.$$

**Proposition 3.2** (*Birch's Theorem*). *The value of an L-series twisted by a Dirichlet character can be expressed as a weighted sum of modular symbols*

$$L(f, 1, \chi) = \frac{\tau(\chi)}{f_{\chi}} \sum_{a \bmod f_{\chi}} \bar{\chi}(a) \left\{ \infty, \frac{a}{f_{\chi}} \right\}$$

where  $\tau(\chi)$  is the Gauss sum.

**Proposition 3.3** (*Hecke action*). *For an eigenform  $f$  of the Hecke operator  $T_p$  with eigenvalue  $a_p$  we have an action on the modular symbol as follows*

$$a_p \left\{ \infty, \frac{a}{f_{\chi}} \right\} = \left\{ \infty, \frac{a}{f_{\chi}} \right\}^{T_p} = \sum_{u=0}^{p-1} \left\{ \infty, \frac{a - u f_{\chi}}{p f_{\chi}} \right\} + \delta(p) \left\{ \infty, \frac{ap}{f_{\chi}} \right\}$$

where  $\delta(p) = 0$  if  $p|N$  and  $\delta(p) = 1$  otherwise.

**Proposition 3.4** (*Integrality*). *There are non-zero complex numbers  $\Omega^{\pm}$  depending only upon  $f$  such that*

$$\Lambda^{\pm}(a, f_{\chi}) := \left( \left\{ \infty, \frac{a}{f_{\chi}} \right\} \pm \left\{ \infty, \frac{-a}{f_{\chi}} \right\} \right) / \Omega^{\pm} \text{ are integers.}$$

*In the case that  $f$  is the cuspform associated to an elliptic curve, then the numbers  $\Omega^{\pm}$  are rational multiples of the periods of the elliptic curve.*

Note that for  $\gamma \in \Gamma_0(N)$ , and  $f \in S_2(\Gamma_0(N))$ , that  $\{\gamma(\alpha), \gamma(\beta)\}f = \{\alpha, \beta\}f$ . It follows that  $\Lambda^\pm(a, \mathfrak{f}_\chi)$  depends only on the residue class of  $a \pmod{\mathfrak{f}_\chi}$ .

Since we consider characters  $\chi$  of prime order  $\ell > 2$ , they will be even characters (i.e.  $\chi(-1) = 1$ ) and we then take the positive sign. In what follows we write  $\Lambda$  for  $\Lambda^+$  and  $\Omega$  for  $\Omega^+$ .

Following Mazur, Tate and Teitelbaum ([MTT]) define the algebraic part of  $L(f, 1, \chi)$  to be

$$\begin{aligned} L^{\text{alg}}(f, 1, \chi) &= \frac{2\mathfrak{f}_\chi L(f, 1, \chi)}{\Omega\tau(\chi)} \\ &= \sum_{a \pmod{\mathfrak{f}_\chi}} \bar{\chi}(a) \Lambda(a, \mathfrak{f}_\chi) \end{aligned}$$

where  $\Omega$  is a non-zero rational multiple of the real period of  $E$  independent of  $\chi$  as above and  $\Lambda(a, \mathfrak{f}_\chi) \in \mathbb{Z}$ .

Let  $\mathfrak{l}$  be a prime dividing  $\ell$  in the cyclotomic field  $\mathbb{Q}(\zeta_\ell)$  of  $\ell$ -th roots of unity and let  $\chi \in \mathcal{X}(\ell)$  be a Dirichlet character with conductor  $\mathfrak{f}_\chi$ . Then

$$\begin{aligned} \chi(a) &\equiv 1 \pmod{\mathfrak{l}} \text{ when } (a, \mathfrak{f}_\chi) = 1 \\ \chi(a) &= 0 \text{ when } (a, \mathfrak{f}_\chi) \neq 1. \end{aligned}$$

So

$$\sum_{a \pmod{\mathfrak{f}_\chi}} \bar{\chi}(a) \Lambda(a, \mathfrak{f}_\chi) \equiv \sum_{\substack{a \pmod{\mathfrak{f}_\chi} \\ (a, \mathfrak{f}_\chi) = 1}} \Lambda(a, \mathfrak{f}_\chi) \pmod{\mathfrak{l}}.$$

Fix a cuspform  $f \in S_2(N)$ , let

$$S_m(t) := \sum_{\substack{a \pmod{t} \\ (a, m) = 1}} \Lambda(a, t).$$

For a character of order  $\ell$  and conductor  $\mathfrak{f}_\chi$  we have

$$L^{\text{alg}}(f, 1, \chi) \equiv S_{\mathfrak{f}_\chi}(\mathfrak{f}_\chi) \pmod{\mathfrak{l}}.$$

**Theorem 3.5.** *Let  $f \in S_2(N)$  be a simultaneous eigenform for all the Hecke operators. Let  $\chi$  be Dirichlet character of order  $\ell$  and conductor  $\mathfrak{f}_\chi$ , and let  $\psi$  be a Dirichlet character of order  $\ell$  and prime conductor  $\mathfrak{f}_\psi = p$  with  $(\mathfrak{f}_\chi, p) = 1$ . Let  $\delta(t) = 1$  if  $(t, N) = 1$  and zero otherwise. Then*

$$L^{\text{alg}}(f, 1, \chi\psi) \equiv (a_p - \delta(p) - 1)L^{\text{alg}}(f, 1, \chi) \pmod{\mathfrak{l}}.$$

If  $\varphi$  is the Dirichlet character of order  $\ell$  and conductor  $\ell^2$  prime to  $\mathfrak{f}_\chi$  we have

$$L^{alg}(f, 1, \chi\varphi) \equiv (a_\ell - 1)(a_\ell - \delta(\ell))L^{alg}(f, 1, \chi) \pmod{\mathfrak{l}}.$$

Since any character  $\psi$  of order  $\ell$  and conductor  $\mathfrak{f}_\psi$  can be factored as a product of characters of order  $\ell$  either with prime conductors, or with conductor  $\ell^2$ , we can iterate the above result to obtain:

**Corollary 3.6.** *For  $f \in S_2(N)$  and  $\chi, \psi \in \mathcal{X}(\ell)$ , if  $\mathfrak{f}_\psi$  is not divisible by  $\ell$  then we have*

$$L^{alg}(f, 1, \chi\psi) \equiv L^{alg}(f, 1, \chi) \prod_{p|\mathfrak{f}_\psi} (a_p - \delta(p) - 1) \pmod{\mathfrak{l}}.$$

or if  $\ell \mid \mathfrak{f}_\psi$

$$L^{alg}(f, 1, \chi\psi) \equiv L^{alg}(f, 1, \chi)(a_\ell - 1)(a_\ell - \delta(\ell)) \prod_{\substack{p|\mathfrak{f}_\psi \\ p \neq \ell}} (a_p - \delta(p) - 1) \pmod{\mathfrak{l}}.$$

*Proof of Theorem 3.5.* We consider the sums  $S_m(m)$ ,  $S_{mp}(mp)$ , and  $S_{mp^2}(mp^2)$ . Assume that  $(m, p) = 1$ .

$$\begin{aligned} S_m(m) \mid T_p &= a_p S_m(m) = \sum_{\substack{a \bmod m \\ (a, m)=1}} \left[ \sum_{u=0}^{p-1} \Lambda(a - um, pm) + \delta(p) \Lambda(ap, m) \right] \\ &= \sum_{\substack{a \bmod m \\ (a, m)=1}} \sum_{u=0}^{p-1} \Lambda(a - um, pm) + \delta(p) \sum_{\substack{a \bmod m \\ (a, m)=1}} \Lambda(ap, m) \\ &= S_m(pm) + \delta(p) S_m(m). \end{aligned}$$

Now

$$\begin{aligned} S_m(pm) &= \sum_{\substack{a \bmod pm \\ (a, m)=1}} \Lambda(a, pm) \\ &= \sum_{\substack{a \bmod pm \\ (a, pm)=1}} \Lambda(a, pm) + \sum_{\substack{a \bmod pm \\ (a, pm)=p}} \Lambda(a, pm) \\ &= S_{pm}(pm) + \sum_{\substack{b \bmod m \\ (b, m)=1}} \Lambda(bp, pm) \end{aligned}$$



$$= S_{pm}(pm) + S_m(m).$$

So

$$a_p S_m(m) = S_{pm}(pm) + S_m(m) + \delta(p) S_m(m)$$

$$S_{pm}(pm) = (a_p - 1 - \delta(p)) S_m(m).$$

Taking  $m = f_\chi$ , and noting that  $f_\psi = p$  we have

$$L^{\text{alg}}(f, 1, \chi^\psi) \equiv S_{pm}(pm) \pmod{\mathfrak{l}}$$

$$L^{\text{alg}}(f, 1, \chi) \equiv S_m(m) \pmod{\mathfrak{l}}.$$

Therefore the first statement of Theorem 3.5 follows:

$$L^{\text{alg}}(f, 1, \chi^\psi) \equiv (a_p - \delta(p) - 1) L^{\text{alg}}(f, 1, \chi) \pmod{\mathfrak{l}}.$$

To treat  $S_{mp^2}(mp^2)$  we apply  $T_p$  a second time.

$$\begin{aligned} (S_m(m) \mid T_p) \mid T_p &= a_p^2 S_m(m) = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left[ \sum_{u=0}^{p-1} \Lambda(a - um, pm)^{T_p} + \delta(p) \Lambda(ap, m)^{T_p} \right] \\ &= \sum_{\substack{a \bmod m \\ (a,m)=1}} \sum_{v=0}^{p-1} \sum_{u=0}^{p-1} \Lambda(a - um - vmp, p^2 m) \\ &\quad + \delta(p) \sum_{\substack{a \bmod m \\ (a,m)=1}} \sum_{v=0}^{p-1} ((a - um)p, pm) \\ &\quad + \delta(p) \sum_{\substack{a \bmod m \\ (a,m)=1}} \sum_{v=0}^{p-1} \Lambda(ap - vm, pm) + \delta^2(p) \sum_{\substack{a \bmod m \\ (a,m)=1}} \Lambda(ap^2, m) \\ &= S_m(mp^2) + \delta(p) p S_m(m) + \delta(p) S_m(pm) + \delta(p) S_m(m). \end{aligned}$$

Now

$$S_m(pm) = S_{pm}(pm) + S_m(m)$$

and

$$\begin{aligned}
S_m(mp^2) &= \sum_{\substack{a \bmod p^2m \\ (a,m)=1}} \Lambda(a, p^2m) \\
&= \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=1}} \Lambda(a, p^2m) + \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=p}} \Lambda(a, p^2m) + \sum_{\substack{a \bmod p^2m \\ (a,mp^2)=p^2}} \Lambda(a, p^2m) \\
&= S_{mp^2}(mp^2) + \sum_{\substack{b \bmod pm \\ (b,mp)=1}} \Lambda(bp, p^2m) + \sum_{\substack{c \bmod m \\ (c,m)=1}} \Lambda(cp^2, p^2m) \\
&= S_{mp^2}(mp^2) + S_{mp}(mp) + S_m(m).
\end{aligned}$$

So

$$\begin{aligned}
a_p^2 S_m(m) &= S_{mp^2}(mp^2) + S_{mp}(mp) + S_m(m) + \delta(p)pS_m(m) + \delta(p)S_m(m) \\
&\quad + \delta(p)(S_{pm}(pm) + S_m(m)) \\
&= S_{mp^2}(mp^2) + S_{mp}(mp)(1 + \delta(p)) + S_m(m)(1 + \delta(p)p + 2\delta(p)) \\
&= S_{mp^2}(mp^2) \\
&\quad + (a_p - 1 - \delta(p))(1 + \delta(p))S_m(m) + S_m(m)(1 + \delta(p)p + 2\delta(p)) \\
&= S_{mp^2}(mp^2) + S_m(m)(a_p + \delta(p)a_p - \delta(p) + \delta(p)p).
\end{aligned}$$

Simplifying

$$\begin{aligned}
S_{mp^2}(mp^2) &= [a_p^2 - a_p - \delta(p)a_p - \delta(p)p + \delta(p)] S_m(m) \\
&= [(a_p - 1)(a_p - \delta(p)) - \delta(p)p] S_m(m).
\end{aligned}$$

Taking  $p = \ell$  we see that the second statement of Theorem 3.5 now follows as above. If  $\varphi$  is the Dirichlet character of order  $\ell$  and conductor  $\ell^2 = p^2$  prime to  $\mathfrak{f}_\chi$  we have

$$\begin{aligned}
L^{\text{alg}}(f, 1, \chi\varphi) &\equiv S_{mp^2}(mp^2) \bmod \mathfrak{l} \\
&\equiv [(a_\ell - 1)(a_\ell - \delta(\ell)) - \delta(\ell)\ell] S_m(m) \bmod \mathfrak{l} \\
&\equiv (a_\ell - 1)(a_\ell - \delta(\ell)) L^{\text{alg}}(f, 1, \chi) \bmod \mathfrak{l}.
\end{aligned}$$

Therefore we see that the central value of a twist of  $L(E, s)$  by a Dirichlet character of conductor  $\mathfrak{f}_\chi$ , with  $(\mathfrak{f}_\chi, N_E) = 1$ , can only vanish  $\bmod \mathfrak{l}$  if either  $L^{\text{alg}}(E, 1) \equiv 0 \pmod{\mathfrak{l}}$  or if one of the factors  $(a_p - \delta(p) - 1)$  or  $(a_\ell - 1)(a_\ell - \delta(\ell))$  vanishes  $\bmod \mathfrak{l}$ .

By Čebotarev's theorem, (see Serre [Ser]) we can find a *positive density* of primes  $p \equiv 1 \pmod{\ell}$  for which the factors  $(a_p - \delta(p) - 1) \not\equiv 0 \pmod{\ell}$ . Therefore we have proved:

**Theorem 3.7.** *Let  $E/\mathbb{Q}$  be an elliptic curve and let  $\ell$  be a prime. Suppose that  $L^{alg}(E, 1) \not\equiv 0 \pmod{\ell}$ , then there is a set of primes,  $S$ , of positive density such that  $L(E, 1, \chi) \neq 0$  for any characters  $\chi$  of order  $\ell$  with conductor  $\mathfrak{f}_\chi$  supported on  $S$ .*

□

The statement of Theorem A follows immediately from Theorem 3.7.

**Theorem 3.8.** *Let  $E/\mathbb{Q}$  be an elliptic curve such that  $L(E, 1) \neq 0$ . Then for all but a finite number of primes  $\ell$ , there is a set of primes  $S_\ell$  of positive density such that  $L(E, 1, \chi) \neq 0$  for all characters  $\chi$  of order  $\ell$  with conductor  $\mathfrak{f}_\chi$  supported on  $S_\ell$ .*

#### 4. VANISHING TWISTS AND RATIONAL POINTS OF AN AUXILIARY VARIETY

Kato's result generalizing Kolyavagin's theorem [Kato] shows that if the  $\chi$ -component of  $E(K_\chi)$  has positive rank, then  $L(E/\mathbb{Q}, 1, \chi) = 0$ . Thus, the algebro-geometric version of our question is whether the  $\chi$ -component  $E(K_\chi)^\chi$  of  $E(K_\chi)$  has positive rank or not, as  $K_\chi$  ranges over the corresponding cyclic extensions of  $\mathbb{Q}$ . In order to find points on  $E$  defined over some cyclic extension  $K_\chi$ , we will define an auxiliary variety of higher dimension whose  $\mathbb{Q}$ -rational points correspond to points on  $E$  defined over some cyclic extensions. The definition of this auxiliary variety can be done in a general context, and thus, we develop a general theory in the following.

Let  $X$  be an algebraic variety defined over a number field  $k$ , namely, a geometrically integral scheme of finite type over  $\text{Spec } k$ . Let  $\bar{k}$  be an algebraic closure of  $k$ , which we fix once and for all. We denote by  $G_k = \text{Gal}(\bar{k}/k)$  its Galois group. Throughout this section, a point means a geometric point, i.e., a  $\bar{k}$ -valued point. This is the same as a closed point of the scheme  $X \times_k \text{Spec } \bar{k}$ .

Let  $G$  be a finite group of order  $n$ . By writing  $G = \{g_1, g_2, \dots, g_n\}$ , we fix a bijection between  $G$  and  $\{1, 2, \dots, n\}$ . The left translation  $L_g : x \mapsto gx$  induces an injective homomorphism from  $G$  to the symmetric group  $\mathfrak{S}_n$ , and we let  $G$  act on

the variety  $X^n = X \times \cdots \times X$  via this homomorphism. More precisely, define a permutation  $\pi_g \in \mathfrak{S}_n$  by the formula  $gg_i = g_{\pi_g(i)}$ , and define an action of  $g \in G$  by

$$g \cdot (P_1, P_2, \dots, P_n) = (P_{\pi_g^{-1}(1)}, P_{\pi_g^{-1}(2)}, \dots, P_{\pi_g^{-1}(n)}).$$

Let  $Y = X^n/G$  be its quotient variety (cf. [Mum, Ch. II, §7 and Ch. III, §12]). It is obvious that the  $G$ -action on  $X^n$  commutes with the Galois action on  $X^n$ . Thus,  $Y$  is a variety defined over  $k$ . We denote by  $[P_1, \dots, P_n]$  the class of  $(P_1, \dots, P_n)$  in  $Y$ .

Let  $(X^n)^\circ$  be the open set of  $X^n$  consisting of points whose stabilizer in  $G$  is reduced to the identity element. The group  $G$  acts on  $(X^n)^\circ$  freely. Let  $Y^\circ$  the quotient of  $(X^n)^\circ$  by  $G$ .

**Lemma 4.1.** *A point  $[P_1, \dots, P_n]$  in  $Y^\circ$  is a  $k$ -rational point if and only if there is a Galois extension  $K$  of  $k$  such that*

- (1) *for all  $i$ ,  $P_i$  is defined over  $K$ , and*
- (2) *there is an injective homomorphism  $\rho : \text{Gal}(K/k) \rightarrow G$  such that*

$$(\sigma(P_1), \dots, \sigma(P_n)) = \rho(\sigma)^{-1} \cdot (P_1, \dots, P_n)$$

*for all  $\sigma \in \text{Gal}(K/k)$ .*

*Proof.* Suppose  $[P_1, \dots, P_n] \in Y^\circ$  is a  $k$ -rational point. This is equivalent to say that for any  $\sigma \in \text{Gal}(\bar{k}/k)$  there exist  $g_\sigma \in G$  such that  $(\sigma(P_1), \dots, \sigma(P_n)) = g_\sigma \cdot (P_1, \dots, P_n)$ . We first claim that  $g_\sigma$  is unique. Indeed, if  $g'_\sigma$  is another element satisfying the same property, then  $g_\sigma^{-1}g'_\sigma$  fixes the point  $(P_1, \dots, P_n)$ . But  $G$  acts freely on  $(X^n)^\circ$ , which implies  $g_\sigma^{-1}g'_\sigma$  is the identity. We thus have a map  $\text{Gal}(\bar{k}/k) \rightarrow G$  given by  $\sigma \mapsto g_\sigma$ . It is easy to see that this is an anti-homomorphism; i.e., we have  $g_{\sigma\tau} = g_\tau g_\sigma$ . Thus we obtain a homomorphism  $\tilde{\rho}$  by defining  $\sigma \mapsto g_\sigma^{-1}$ .

Let  $\text{Stab}_k(P_i)$  denote the stabilizer  $\text{Gal}(\bar{k}/k)$  on  $X$ . We claim that  $\text{Stab}_k(P_1) = \text{Stab}_k(P_2) = \cdots = \text{Stab}_k(P_n)$ . To show this choose  $h \in G$  such that  $g_1 = hg_i$ , and let  $\tau$  be any element of  $\text{Stab}_k(P_1)$ . Then the first coordinate of  $\tau h(P_1, \dots, P_n)$  is  $\tau(P_i)$ , while the first coordinate of  $h\tau(P_1, \dots, P_n)$  is  $P_i$ . Since  $\tau$  and  $h$  commute, we deduce that  $\tau(P_i) = P_i$ . This shows that  $\text{Stab}_k(P_1)$  is contained in  $\text{Stab}_k(P_i)$ . Exchanging the roles of 1 and  $i$ , the same argument shows that  $\text{Stab}_k(P_i)$  is also

contained in  $\text{Stab}_k(P_1)$ . This shows that  $\text{Stab}_k(P_1) = \text{Stab}_k(P_i)$  for any  $i$ . It follows that  $\text{Stab}_k(P_i)$  is the kernel of the  $\text{Gal}(\bar{k}/k)$ -action on the set  $\{P_1, \dots, P_n\}$ . In particular,  $\text{Stab}_k(P_i)$  is a normal subgroup of finite index in  $\text{Gal}(\bar{k}/k)$ . This implies that there is a Galois extension  $K/k$  such that  $\text{Stab}_k(P_i) = \text{Gal}(\bar{k}/K)$ . This means that  $P_i$  is defined over  $K$  for all  $i$ . Since  $\text{Stab}_k(P_i)$  is also the kernel of the homomorphism  $\tilde{\rho}$ , we have an injective homomorphism  $\rho : \text{Gal}(K/k) \simeq \text{Gal}(\bar{k}/k) / \text{Gal}(\bar{k}/K) \rightarrow G$  induced by  $\tilde{\rho}$ . This homomorphism  $\rho$  satisfies the condition (2).  $\square$

Next we consider the case where  $X$  is an abelian variety  $A$ . For any  $X$ , the diagonal  $D = \{(P, P, \dots, P) \mid P \in X\}$  of  $X^n$  is a subvariety on which  $G$  acts trivially. If  $X = A$  is an abelian variety (or more generally, a commutative group variety), then  $D$  is a subgroup of  $A^n$ , and we may define the complement  $\hat{D}$  of  $D$  in  $A^n$  to be

$$\hat{D} = \{(P_1, P_2, \dots, P_n) \mid \sum_{i=1}^n P_i = O\}.$$

Then  $\hat{D}$  is a subgroup of  $A^n$  invariant under  $G$ -action. We have  $(D \times \hat{D})/G = D \times (\hat{D}/G) \simeq A \times (\hat{D}/G)$ . Moreover we have a degree  $n$  isogeny  $\varphi$  given by

$$\begin{aligned} \varphi : \quad A^n &\longrightarrow D \times \hat{D} \\ (P_1, \dots, P_n) &\longmapsto \left( \left( \sum_{i=1}^n P_i, \dots, \sum_{i=1}^n P_i \right), \left( nP_1 - \sum_{i=1}^n P_i, \dots, nP_n - \sum_{i=1}^n P_i \right) \right). \end{aligned}$$

Its dual isogeny  $\varphi' : D \times \hat{D} \rightarrow A^n$  is given by

$$\begin{aligned} \varphi' : \quad D \times \hat{D} &\longrightarrow A^n \\ ((R, \dots, R), (P_1, \dots, P_n)) &\longmapsto (P_1 + R, \dots, P_n + R). \end{aligned}$$

Since  $\varphi$  and  $\varphi'$  commute with the  $G$ -action, we take the quotients by the  $G$ -action and obtain two maps

$$\bar{\varphi} : Y \rightarrow A \times (\hat{D}/G), \quad \bar{\varphi}' : A \times (\hat{D}/G) \rightarrow Y$$

such that  $\bar{\varphi}' \circ \bar{\varphi}$  is the map  $\overline{[n]}$  induced from the multiplication-by- $n$  map  $[n]$  of  $A^n$ .

**Remark 4.2.** Just as the regular representation of  $G$  decomposes to a direct sum of irreducible representations, the permutation action of  $G$  on  $A^n$  decomposes to a direct product of abelian varieties with irreducible  $G$  actions, though the decomposition is only up to isogeny.

## 5. VANISHING OF CUBIC TWISTS

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . The goal of this section is to prove Theorem B. To do so, we will prove its algebro-geometric version Theorem B' and then apply Kato's theorem to conclude the vanishing of the corresponding twisted  $L$ -functions.

**Theorem B'.** *Let  $E$  be an elliptic curve defined over a number field  $k$ . Suppose that there is at least one cyclic extension  $K_0/k$  of degree dividing 3 such that  $E(K_0)$  is infinite (possibly  $K_0 = k$ ). Then  $\text{rank}_{\mathbb{Z}} E(K_\lambda) > \text{rank}_{\mathbb{Z}} E(k)$  for infinitely many cyclic cubic extensions  $K_\lambda/k$ .*

In order to prove Theorem B', we apply the results of the previous section to the case where  $X = E$ , and  $G$  is the symmetric group  $\mathfrak{S}_3$  or its alternating sub group  $\mathfrak{A}_3$ , which is a cyclic group of order 3.

Let  $\widehat{D} = \{(P, Q, R) \mid P + Q + R = O\} \subset E^3$ .  $\mathfrak{S}_3$  acts on  $E^3$  in an obvious way and  $\widehat{D}$  is stable under this action. We have the maps

$$\widehat{D} \longrightarrow \widehat{D}/\mathfrak{A}_3 \longrightarrow \widehat{D}/\mathfrak{S}_3.$$

We denote the surace  $\widehat{D}/\mathfrak{A}_3$  by  $\overline{S}_E$ .

**Lemma 5.1.** *The set of  $k$ -rational points of  $\overline{S}_E$  consists of points of the form:*

- (1)  $[P, Q, R]$ , where  $P, Q, R \in E(k)$  and  $P + Q + R = O$ , or
- (2)  $[P, P^\sigma, P^{\sigma^2}]$ , where  $P$  is a point defined over a certain cyclic cubic extension  $K/k$  satisfying the relation  $P + P^\sigma + P^{\sigma^2} = O$ , where  $\sigma$  is a generator of its Galois group  $\text{Gal}(K/k)$ .

*Proof.* If  $[P, Q, R]$  is not the image of a fixed point of the  $\mathfrak{A}_3$ -action, then the assertion follows from Lemma 4.1. A fixed point of the  $\mathfrak{A}_3$ -action is of the form  $[P, P, P]$  with  $3P = O$ .  $[P, P, P]$  is defined over  $k$  if and only if  $P$  is defined over  $k$ . So, this is included in the first case.  $\square$

Let  $K/k$  be any finite extension and let  $\text{Tr}_{K/k} : E(K) \rightarrow E(k)$  denote the trace map. The kernel  $\text{Ker } \text{Tr}_{K/k} \subset E(K)$  is the subgroup of points of  $E(K)$  of trace zero. The point satisfying the second condition of Lemma 5.1 belongs to  $\text{Ker } \text{Tr}_{K/k}$ .

**Lemma 5.2.** *The following are equivalent:*

- (1)  $\text{rank}_{\mathbb{Z}} E(K) > \text{rank}_{\mathbb{Z}} E(k)$ ,
- (2)  $E(K)$  contains a trace zero point of infinite order,
- (3)  $\#(\text{Ker } \text{Tr}_{K/k}) = \infty$ .

*Proof.* Define the maps  $t$  and  $t'$  of abelian groups as follows.

$$\begin{array}{ccc}
 E(K) & \xrightarrow{t} & E(k) \times \text{Ker } \text{Tr}_{K/k} & \xrightarrow{t'} & E(K) \\
 P & \longmapsto & (\text{Tr}_{K/k}(P), nP - \text{Tr}_{K/k}(P)) & & \\
 & & (Q, R) & \longmapsto & Q + R
 \end{array}$$

Then we see that  $t' \circ t = [n]$  and  $t \circ t' = [n]$ , where  $[n]$  is the multiplication-by- $n$  map. Thus, we have

$$\text{rank}_{\mathbb{Z}} E(K) = \text{rank}_{\mathbb{Z}} E(k) + \text{rank}_{\mathbb{Z}} \text{Ker } \text{Tr}_{K/k}.$$

The statement of Lemma follows immediately.  $\square$

In order to give a concrete description of  $\widehat{D}/\mathfrak{S}_3$ , we fix a Weierstrass model of  $E$  and consider it as a curve in  $\mathbb{P}^2$ . Namely, suppose that  $E$  is given by the equation

$$E : y^2 z + a_1 x y z + a_3 y z^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3.$$

Then, as is well known, three points  $P, Q$  and  $R$  satisfy  $P + Q + R = O$  if and only if  $P, Q$  and  $R$  are collinear. Let  $(\mathbb{P}^2)^*$  be the dual space of  $\mathbb{P}^2$ , namely, the space of all the lines in  $\mathbb{P}^2$ . For a point  $(P, Q, R) \in \widehat{D}$  we denote by  $\ell_{PQR}$  the line passing through  $P, Q$  and  $R$ . If  $P = Q = R$ , we understand that  $\ell_{PPP}$  is the tangent line to  $E$  passing through  $P$ . Consider the map

$$\begin{array}{ccc}
 \pi_0 : & \widehat{D} & \longrightarrow (\mathbb{P}^2)^* \\
 & (P, Q, R) & \longmapsto \ell_{PQR}.
 \end{array}$$

It is clear that  $\pi_0$  is surjection and is invariant under the  $\mathfrak{S}_3$ -action. Thus we obtain an isomorphism  $\widehat{D}/\mathfrak{S}_3 \xrightarrow{\sim} (\mathbb{P}^2)^*$ , which sends a class  $[P, Q, R]$  of  $\widehat{D}/\mathfrak{S}_3$  to the line  $\ell_{PQR}$ . Now,  $\pi_0$  induces the map

$$\pi_1 : \overline{S}_E = \widehat{D}/\mathfrak{A}_3 \longrightarrow \widehat{D}/\mathfrak{S}_3 \simeq (\mathbb{P}^2)^*.$$

$\pi_0$  is a covering map of degree  $2 = [\mathfrak{S}_3 : \mathfrak{A}_3]$ . It is easy to see that  $\pi_1^{-1}(\ell_{PQR})$  consists of two classes,  $[P, Q, R]$  and  $[P, R, Q]$ . In  $\overline{S}_E$  the classes  $[P, Q, R]$  and  $[P, R, Q]$  coincide if and only if at least two of three points coincide. In other words  $[P, Q, R] = [P, R, Q]$  if and only if  $\ell_{PQR}$  is a tangent line to the curve  $E$ . This

implies that the double covering  $\pi_1$  ramifies along the dual curve  $E^* = \{L \in (\mathbb{P}^2)^* \mid L \text{ is tangent to } E\}$ .  $E^*$  is an irreducible curve of degree 6, and it has nine cusps corresponding to the tangent lines at nine inflection points of  $E$ . The surface  $\overline{S}_E$  thus have nine singular points of type  $A_2$ . Let  $S_E$  be the minimal desingularization of  $\overline{S}_E$  obtained by blowing up twice at each singular points. Summing all up, we have

**Proposition 5.3.** *The quotient surface  $\overline{S}_E = \widehat{D}/\mathfrak{A}_3$  may be regarded as a double cover of the dual projective plane  $(\mathbb{P}^2)^*$  ramifying along the dual curve of  $E$ , which is an irreducible curve of degree 6. As a consequence the minimal desingularization  $S_E$  of  $\overline{S}_E$  is a K3 surface.*  $\square$

**Remark 5.4.** If the quotient of an abelian surface  $A$  by a finite group  $G$  is birational to a K3 surface, then its minimal desingularization is called a generalized Kummer surface.  $S_E$  is thus a generalized Kummer surface. For more about Kummer surfaces see Katsura[Kat] and Bertin[Ber].

Write the equation of a generic line  $\ell$  in  $\mathbb{P}^2$  in the form  $y = tx + u$ , using parameters  $t$  and  $u$ . The function field of  $(\mathbb{P}^2)^*$  is then given by  $k(t, u)$ , and the function field of  $\widehat{D}$  can be regarded as the splitting field of the cubic equation in  $x$  obtained by substituting  $y = tx + u$  in the affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The function field of  $\overline{S}_E = \widehat{D}/\mathfrak{A}_3$  is then the extension of  $k(t, u)$  obtained by adding the square root of the discriminant  $\Delta(u, t)$  of this cubic equation with respect to  $x$ . This implies that the surface  $S_E$  is a minimal model of the surface defined by the equation

$$\delta^2 = \Delta(u, t).$$

For simplicity we write the explicit result only in the case where  $a_1 = a_2 = a_3 = 0$ ,  $a_4 = A$ , and  $a_6 = B$ .

**Proposition 5.5.** *Suppose that an elliptic curve  $E$  is given by the Weierstrass equation  $y^2 = x^3 + Ax + B$ . Then the generalized Kummer surface  $S_E$  is birational to the affine surface in  $\mathbb{A}^3 = \{(t, u, \delta)\}$  defined by the equation*

$$(1) \quad \delta^2 = -27u^4 - 4t^3u^3 - (30At^2 - 54B)u^2 - 4t(At^4 - 9t^2 - 6A^2)u \\ + 4Bt^6 + A^2t^4 - 18ABt^2 - (4A^3 + 27B^2). \quad \square$$



**Remark 5.6.** The surface  $S_E$  possesses two obvious involutions,  $[P, Q, R] \mapsto [Q, P, R]$  and  $[P, Q, R] \mapsto [-P, -Q, -R]$ . In terms of the equation (1) the former corresponds to  $(t, u, \delta) \mapsto (t, u, -\delta)$ , while the latter corresponds to  $(t, u, \delta) \mapsto (-t, -u, \delta)$ .

Consider the map  $\nu : E \rightarrow \overline{S}_E$  given by  $P \mapsto [P, -P, O]$ . This is an injection, and we have an embedding  $\tilde{\nu} : E \rightarrow S_E$ . Let  $D_{\tilde{\nu}(E)}$  be the divisor associated with the image of  $\tilde{\nu}$ . Then the complete linear system  $|D_{\tilde{\nu}(E)}|$  determines a pencil of curves of genus 1. Let  $\bar{\pi} : \overline{S}_E \rightarrow \mathbb{P}^1$  be the map associated with the projection  $(t, u, \delta) \mapsto t$ . The fiber at  $t = \infty$  corresponds exactly the image of the embedding  $P \mapsto [P, -P, O]$ , and thus the fibration  $\pi$  coincides with the pencil above. Let  $\pi : S_E \rightarrow \mathbb{P}^1$  be the elliptic fibration obtained in this way.

Let  $C_t$  be the fiber of  $\pi$  at the generic point  $t$  of  $\mathbb{P}^1$ . This is nothing but the curve of genus 1 defined over the function field  $k(t)$  given by the equation (1).

The coefficient of  $u^4$  in the right-hand side of (1) is constant, namely,  $-27$ . Thus, the curve  $C_t$  has two points at infinity defined over  $k(\sqrt{-3})$ . In other words, if  $k$  contains  $\sqrt{-3}$ ,  $C_t$  has a  $k(t)$ -rational point and it is an elliptic curve over  $k(t)$ . However, if  $k$  does not contain  $\sqrt{-3}$ , we do not know if  $C_t$  has a  $k(t)$ -rational point, and if we can consider it as an elliptic curve. Instead, we need to consider its Jacobian  $J_t$ .

Using an algorithm for calculating an equation of the Jacobian of the curve given by a quartic equation (see Connell[Con]), we see that  $J_t$  is given by the equation

$$\begin{aligned} J_t : Y^2 = X^3 &+ (At^8 + 18Bt^6 - 18A^2t^4 - 54ABt^2 - 27(A^3 + 9B^2))X \\ &+ (Bt^{12} - 4A^2t^{10} - 45ABt^8 - 270B^2t^6 + 135A^2Bt^4 \\ &\quad - 54A(2A^3 + 9B^2)t^2 - 243B(A^3 + 6B^2)). \end{aligned}$$

**Proposition 5.7.** *The elliptic surface associated with the curve  $J_t$  has eight singular fibers of type  $I_3$  located at  $t$  satisfying*

$$(2) \quad t^8 + 18At^4 + 108Bt^2 - 27A^2 = 0.$$

*The Mordell-Weil group  $J_t(\bar{k}(t))$  contains an point of infinite order  $\gamma_1$  given by*

$$\gamma_1 = \left( -\frac{1}{27}t^6 + 5At^2 - 9B, \frac{\sqrt{-3}}{243}t(t^8 + 162At^4 - 2916Bt^2 - 2187A^2) \right).$$

*Proof.* It is easy to determine the singular fibers using Tate's algorithm. Over  $k(\sqrt{-3})$ ,  $C_t$  and  $J_t$  are isomorphic. Using an algorithm in [Con], we can write an isomorphism which send one of the two points at infinity on  $C_t$  to the origin of  $J_t$  and the other to  $\gamma_1$ . Using an algorithm in [Kuw], we calculate the height of  $\gamma_1$ , which turns out to be 3. This implies that it has infinite order.  $\square$

**Remark 5.8.** We note that, if  $E$  does not have complex multiplication, then  $J_t(\bar{k}(t))$  is isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},$$

and  $J_t(\bar{k}(t))/J_t(\bar{k}(t))_{\text{tors}}$  is generated by  $\gamma_1$ . All the points in  $J_t(\bar{k}(t))$  are defined already over  $k(E[3])(t)$ . We omit the proof since we do not need these facts in the sequel.

**5.1. Proof of Theorem B'.** We begin by proving some lemmas that are necessary later in the proof.

Consider the surface defined by (1) together with the fibration  $(t, u, \delta) \mapsto t$ . Suppose we have infinitely many  $k$ -rational points  $\gamma_n = (u_n, t_0, \delta_n)$  for a fixed  $t_0$ . For each  $n$ , the point  $\gamma_n$  corresponds to a class  $[P_n, Q_n, R_n]$  in  $S_E$ . Let  $K_n$  be the field over which  $P_n$ ,  $Q_n$  and  $R_n$  are defined. We already know that  $K_n = k$  or  $K_n/k$  is a cyclic cubic extension of  $k$ .

**Lemma 5.9.** *Suppose there is a nonzero  $t_0$  such that the fiber  $C_{t_0} = \pi^{-1}(t_0)$  is a good fiber having infinitely many  $k$ -rational points  $\gamma_n = (u_n, t_0, \delta_n)$ . Then the compositum of all  $K_n$  is an infinite extension of  $k$ .*

*Proof.* For each  $n$ , the cubic polynomial  $x^3 + Ax + B - (t_0x + u_n)^2$  in  $x$  factors into three linear terms over  $K_n$ . Conversely, finding a  $k$ -rational point  $(u, t_0, \delta)$  on the surface (3) is finding  $u$  in  $k$  such that  $x^3 + Ax + B - (tx + u)^2$  factors completely over some cubic cyclic field  $L$ . This is equivalent to finding a point  $(\xi_1, \xi_2, \xi_3, t)$  on the curve given by

$$\begin{cases} \xi_1 + \xi_2 + \xi_3 = t^2, \\ \xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1 = A - 2tu, \\ \xi_1\xi_2\xi_3 = u^2 - B. \end{cases}$$

By eliminating  $\xi_3$  and  $u$ , we obtain a plane curve of degree 4. A calculation shows that this degree 4 curve is nonsingular if and only if  $t_0 \neq 0$  and  $t^8 + 18At^4 +$

$108Bt^2 - 27A^2 \neq 0$ . If that is the case, the genus of the curve is 3. Thus, by a theorem of Faltings, it has only finitely many  $K$ -rational points for each fixed number field  $K$ . Therefore, the compositum of all  $K_n$  cannot be a number field of finite degree over  $\mathbb{Q}$ .  $\square$

In the case where  $k$  contains  $\sqrt{-3}$ , Lemma 5.9 and Proposition 5.7 proves the following statement, which is stronger than Theorem B'.

**Theorem 5.10.** *Let  $E$  be an elliptic curve defined over a number field  $k$  containing  $\sqrt{-3}$ . Then there exist infinitely many cyclic cubic extensions  $K_\lambda$  such that the rank of the Mordell-Weil group  $\text{rank}_{\mathbb{Z}} E(K_\lambda) > \text{rank}_{\mathbb{Z}} E(k)$ .*  $\square$

For the general case we need another lemma.

**Lemma 5.11.** *Let  $S$  be a smooth surface and  $C$  a smooth curve both defined over  $k$ . Let  $\pi : S \rightarrow C$  be a fibration defined over  $k$  such that the generic fiber is a curve of genus 1 equipped with an involution  $\iota$  with a fixed point. Suppose that the set of  $k$ -rational points,  $S(k)$ , is Zariski dense in  $S$ , then there exist infinitely many  $k$ -rational points  $P$  on  $C$  such that the fiber  $\pi^{-1}(P)$  contains infinitely many  $k$ -rational points.*

*Proof.* Let  $\pi' : J \rightarrow C$  be the Jacobian fibration associated with  $\pi : S \rightarrow C$ . There is a map  $f : S \rightarrow J$  of degree 4 defined over  $k$  sending a point  $P \in S$  to the divisor class  $(P) - (\iota(P))$ . Since  $f$  is dominant, the image of  $S(k)$  by  $f$  is Zariski dense.

By Merel's theorem on the bound for the torsion points defined over a number field on an elliptic curve ([Mer]), the set consisting of all the  $k$ -rational torsion points of all the fibers is contained in a proper Zariski closed set. Thus if we denote by  $f(S(k))'$  the set consisting of all the points in the image of  $f(S(k))$  that have infinite order, then  $f(S(k))'$  is still Zariski dense in  $J$ . This means that there are infinitely many  $k$ -rational points  $P$  on  $C$  such that the fiber  $\pi'^{-1}(P)$  contains points in  $f(S(k))'$ . For such  $P$  the  $\pi^{-1}(P)$  contains infinitely many  $k$ -rational points.  $\square$

*Proof of Theorem B'.* Let  $K_0/k$  be a cyclic extension of degree dividing 3 such that  $E(K_0)$  is infinite. Let  $P \in E(K_0)$  be a point of infinite order. First, we show that the set of  $k$ -rational points in  $S_E$  is Zariski dense in  $S_E$ .

If  $K_0 = k$  and  $P$  is defined already over  $k$ , then consider the set  $\{[mP, nP] \mid n, m \in \mathbb{Z}\}$ . This is clearly a Zariski dense set in  $E \times E$ . We thus assume that  $K_0/k$  is a cubic extension and  $P$  is defined over  $K_0$ , but not over  $k$ . Let  $\sigma$  be a generator of  $\text{Gal}(K_0/k)$ . Then  $R = \text{Tr}_{K_0/k}(P)$  is a point defined over  $k$ . If  $R$  is a point of infinite order, then we are in the previous case. If not, replacing  $P$  by  $nP$  if necessary, we may assume that  $\text{Tr}_{K_0/k}(P) = O$ .

We consider  $E(K_0)$  as an  $\text{End}_k(E)$ -module, and we claim that  $P$  and  $P^\sigma$  are  $\text{End}_k(E)$ -linearly independent, except when  $E$  has complex multiplication over  $\mathbb{Q}(\sqrt{-3})$  and  $k$  contains  $\sqrt{-3}$ . Suppose  $[\alpha]$  and  $[\beta]$  two nonzero endomorphisms of  $E$  defined over  $k$ , and suppose we have the relation

$$(3) \quad [\alpha]P + [\beta]P^\sigma = O.$$

Apply  $\sigma$  to both sides of (3). Since  $\sigma$  commutes with  $[\alpha]$  and  $[\beta]$ , we have another relation

$$(4) \quad [\alpha]P^\sigma + [\beta](-P - P^\sigma) = O.$$

Eliminating  $P^\sigma$  from (3) and (4), we obtain

$$([\alpha]^2 + [\alpha][\beta] + [\beta]^2)P = O.$$

This occurs only when  $E$  has complex multiplication by  $\mathbb{Q}(\sqrt{-3})$ . Moreover, since  $[\alpha]$  is defined over  $k$ ,  $\sqrt{-3}$  must be contained in  $k$ . We thus verified the claim. The case where  $k$  contains  $\sqrt{-3}$  has been treated already. In what follows we assume  $\sqrt{-3} \notin k$ .

Next we claim that the subgroup  $\{(nP, nP^\sigma, nP^{\sigma^2}) \mid n \in \mathbb{Z}, P + P^\sigma + P^{\sigma^2} = O\}$  is Zariski dense in  $\widehat{D}$ . To do so, it suffices to show that  $\{(nP, nP^\sigma) \mid n \in \mathbb{Z}\}$  is Zariski dense in  $E \times E$ . Let  $F$  be the Zariski closure of this subgroup. Suppose  $F$  does not equal  $E \times E$ , then  $F$  is a closed subgroup of dimension 1 in  $E \times E$ . Let  $F^0$  be the connected component of  $F$  containing the identity. We then have two isogenies  $\phi_1$  and  $\phi_2$  from  $F^0$  to  $E$ , corresponding to two projections  $E \times E \rightarrow E$ . Choose  $m \in \mathbb{Z}$  such that  $(mP, mP^\sigma)$  is in  $F^0$ . Let  $\hat{\phi}_1$  be the dual isogeny of  $\phi_1$ . Consider the endomorphism  $\phi_2\hat{\phi}_1$  of  $E$ . Let  $d$  be the degree of  $\phi_1$ . Since  $\hat{\phi}_1\phi_1$  equals the

multiplication-by- $d$  map, we have

$$\begin{aligned}\phi_2\hat{\phi}_1(mP) &= \phi_2\hat{\phi}_1\phi_1((mP, mP^\sigma)) \\ &= \phi_2((dmP, dmP^\sigma)) \quad (d = \deg \phi_1) \\ &= dmP^\sigma.\end{aligned}$$

This contradicts the independence of  $P$  and  $P^\sigma$ .

Since the projection map  $\hat{D} \rightarrow \overline{S}_E$  is a dominant map, the set  $\{[nP, nP^\sigma, nP^{\sigma^2}] \mid n \in \mathbb{Z}, P + P^\sigma + P^{\sigma^2}\}$  is also Zariski dense in  $S_E$ . We thus proved that  $S_E(k)$  is Zariski dense in all cases.

The fibration  $\pi : \overline{S}_E \rightarrow \mathbb{P}^1$  constructed in §5.2 satisfies the hypotheses of Lemma 5.11. Thus, there exist infinitely many  $t \in \mathbb{P}^1$  such that the fiber  $\pi^{-1}(t)$  has infinitely many  $k$ -rational points. In particular, we have at least one such  $t$  such that  $t \neq 0$  and  $\pi^{-1}(t)$  is a good fiber. Then Lemma 5.9 implies that there exist infinitely many different cyclic cubic extension  $K_\lambda$  such that the elliptic curve  $E$  possesses a point  $P_\lambda$  defined over  $K_\lambda$ .

In order to complete the proof we have to show that  $P_\lambda$  has infinite order except for finite number of  $\lambda$ . But this is true because the bound of the order of torsion points given by Merel's theorem depends only on the degree of the field.  $\square$

## 6. ELLIPTIC CURVES WITH AT LEAST 6 RATIONAL TORSION POINTS

In this section we prove the following statement.

**Theorem 6.1.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . Suppose that there are at least 6 points in  $E(\mathbb{Q})$ . Then, for infinitely many cyclic cubic extensions  $K/k$ , we have  $\text{rank}_{\mathbb{Z}} E(K) > \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$ .*

*Proof.* If  $E(\mathbb{Q})$  has infinitely many points, then this is nothing but TheoremB'. Suppose  $E(\mathbb{Q})$  is finite. Then, by Mazur's bound for the torsion of elliptic curve over  $\mathbb{Q}$ , either  $E(\mathbb{Q})$  is a cyclic group of order 6, 7, 8, 9, 10, 12, or it contains  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  as a subgroup. In view of Lemma 5.9, it suffices to show that one of the fibers  $C_{t_0}$  of the fibration defined by (1) has infinitely many rational points. In the sequel, we work out in detail to give a particular fiber that have infinitely many rational points for the case where  $E(\mathbb{Q})$  has a point of order 6, or  $E(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . In the case of higher torsion points, we can prove it similarly to the 6-torsion case.

The actual calculations, however, become more complicated, and so we omit it here.  $\square$

**6.1. Elliptic curve with 6-torsion point.** Let us consider the universal elliptic curve having a point of order 6. It is given by the equation

$$y^2 + (1 - \lambda)xy - \lambda(\lambda + 1)y = x^3 - \lambda(\lambda + 1)x^2.$$

When  $\lambda \neq 0, -1$  or  $-1/9$ , this is an elliptic curve and the point  $P = (0, 0)$  is a point of order 6. The line passing through  $P$ ,  $2P$  and  $3P$  is given by  $y = \lambda x$ . Consider the surface in  $\mathbb{A}^2 = \{(t, u, \delta)\}$  with the fibration  $\pi : (t, u, \delta) \mapsto t$  and with parameter  $\lambda$ :

$$\delta^2 = \Delta((tx + u)^2 + (1 - \lambda)x(tx + u) + \lambda(\lambda + 1)(tx + u) - x^3 + \lambda(\lambda + 1)x^2),$$

where  $\Delta(f)$  stands for the discriminant of  $f$  with respect to  $x$ .

We show that the fiber at  $t_0 = \lambda$  has infinitely many rational points. First, we see that it has two points  $(u, \delta) = (0, \pm\lambda^4(\lambda + 1))$  corresponding to the line  $y = \lambda x$  we mentioned above. Choosing one of them, say  $(0, -\lambda^4(\lambda + 1))$ , as the origin, we can convert the equation of the fiber  $C_\lambda = \pi^{-1}(\lambda)$  into Weierstrass form using the method described in Connell[Con]:

$$\begin{aligned} (5) \quad C_\lambda : y^2 + (8\lambda + 2\lambda^2 + 2)xy - 4\lambda(7\lambda + 1)(\lambda - 2)(\lambda + 1)^2y \\ = x^3 - 2\lambda(\lambda + 1)(2\lambda^2 - 4 - \lambda)x^2 + 108\lambda^4(\lambda + 1)^2x \\ - 216\lambda^5(2\lambda^2 - 4 - \lambda)(\lambda + 1)^3. \end{aligned}$$

$C_\lambda$  is an elliptic curve if and only if  $\lambda$  satisfies

$$\lambda(1 + 9\lambda)(2\lambda + 1)(\lambda + 1)(\lambda^4 + 3\lambda^3 + 4\lambda^2 + 1) \neq 0.$$

The point  $(0, \lambda^4(\lambda + 1))$  is sent to the point  $\gamma_1 = (2\lambda(\lambda + 1)(2\lambda^2 - 4 - \lambda), 0)$ .

**Lemma 6.2.** *For all  $\lambda \in \mathbb{Q}$  such that  $C_\lambda$  is an elliptic curve, the point  $(2\lambda(\lambda + 1)(2\lambda^2 - 4 - \lambda), 0)$  is a point of infinite order. When  $\lambda = -1/2$ , then  $C_\lambda$  is not an elliptic curve, but  $(3/2, 0)$  is still a point of infinite order.*

*Proof.* We consider  $C_\lambda$  as the curve defined over  $\mathbb{Q}(\lambda)$ , and calculate  $n\gamma_1$ ,  $n = 1, 2, \dots, 10, 12$ . For all those  $n$  we observe that the denominator of the  $x$ -coordinate

of  $n\gamma_1$  does not vanish for any value of  $\lambda$  except for  $\lambda = 0$ . For  $\lambda = -1/2$ , the group is isomorphic to  $\mathbb{Q}^\times$ . Thus, it suffices to see that it is not a 2-torsion point.  $\square$

**6.2. Elliptic curves with  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  torsion.** The elliptic curve

$$y^2 = x(x + \mu^2)(x + \lambda^2)$$

is the universal elliptic curve with  $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  torsion ([Knapp]). Without loss of generality we may set  $\mu = 1$  giving

$$E_\lambda : y^2 = x(x + 1)(x + \lambda^2)$$

with 4-torsion points

$$\pm P = (s, \pm s(1 + s)), \quad \pm P' = (-s, \pm s(1 - s))$$

and 2-torsion points

$$[2]P = (0, 0), \quad [2]P' = (-1, 0), \quad Q = (-s^2, 0).$$

$E_\lambda$  is an elliptic curve for all  $\lambda$  different from  $\lambda = 0, \pm 1$ .

Intersecting this curve with the line  $y = u + tx$  gives a cubic equation  $(tx + u)^2 = x(x + 1)(x + \lambda^2)$ . Consider the surface in  $\mathbb{A}^2 = \{(t, u, \delta)\}$  with the fibration  $\pi : (t, u, \delta) \mapsto t$  and with parameter  $\lambda$ :

$$\delta^2 = \Delta((tx + u)^2 - x(x + 1)(x + \lambda^2)),$$

where  $\Delta(f)$  is again the discriminant of  $f$  with respect to  $x$ .

For this case we show that the fiber  $t_0 = 1$  has infinitely many points. Setting  $t = 1$  and  $u = \lambda^2$ , the line  $y = x + \lambda^2$  passes through three torsion points

$$P = (\lambda, \lambda(1 + \lambda)), \quad Q = (-\lambda^2, 0), \quad -P - Q = (-\lambda, -\lambda(1 - \lambda)).$$

This triple of points gives rise to rational points  $(\lambda^2, \pm 2\lambda^3(\lambda^2 - 1))$  in  $C_1$ , and we may proceed to convert the curve to Weierstrass form using the method described in Connell[Con]. We then simplify it to obtain

$$\begin{aligned} C_1 : y^2 = x^3 + 27\lambda^2(7\lambda^4 - \lambda^6 + 5\lambda^2 - 27)x \\ + 27\lambda^2(2\lambda^{10} - 21\lambda^8 + 204\lambda^6 - 826\lambda^4 + 1242\lambda^2 - 729), \end{aligned}$$

and a rational point

$$(3(\lambda^4 + 16\lambda^2 + 3), \pm 27(7\lambda^4 + 10\lambda^2 - 1)).$$

The discriminant of  $C_1$  is

$$-2^4 3^{12} \lambda^4 (\lambda - 1)^2 (\lambda + 1)^2 (3\lambda^4 - 14\lambda^2 + 27)^3.$$

**Lemma 6.3.** *For all  $\lambda \in \mathbb{Q}$  different from  $0, \pm 1$ , the curve  $C_1$  is an elliptic curve and point  $(3(\lambda^4 + 16\lambda^2 + 3), \pm 27(7\lambda^4 + 10\lambda^2 - 1))$  is a point of infinite order.*

*Proof.* Considering the fiber  $C_1$  as a curve over  $\mathbb{Q}(\lambda)$ , this point is a point of infinite order, which can be verified by a hight calculation. Just as the case of 6-torsion points,  $C_1$  has a infinitely many rational points for all  $\lambda \neq 0$ . For  $\lambda = \pm 1$ , the group is isomorphic to  $\mathbb{Q}^\times$ . Thus, it suffices to see that it is not a 2-torsion point.  $\square$

## 7. AN EXAMPLE - THE CURVE $E 37B$ .

We now consider one of the curves of conductor 37 which is denoted  $37B$  in Antwerp Table [Ant], and which has Weierstrass equation

$$E 37B : y^2 + y = x^3 + x^2 - 3x + 1.$$

(In Cremona's tables [Cre], it is denoted  $37B3$ .) We decided to study this example because the computations of [Fea] indicated an unusually large number of twists by cubic characters  $\chi$  for which  $L(E 37B, 1, \chi) = 0$ .

Substituting  $(x, y)$  by  $(x + 1, y + 2x)$  in the equation above, we obtain another model of  $E 37B$ :

$$E : y^2 + 4xy + y = x^3.$$

Note that  $(0, 0)$  is a point of order 3. Intersecting the line  $y = tx + u$  with this curve  $E$ , we obtain an affine model of  $\overline{S}_E : \delta^2 = \Delta(u, t)$  with the fibration  $(t, u, \delta) \mapsto t$ . The fiber at  $t = 0$  is a singular fiber given by the equation

$$\delta^2 = -u^2(27u^2 - 202u + 27).$$

This curve has a  $\mathbb{Q}$ -rational parametrization if and only if  $-(27u^2 - 202u + 27)$  is a square for some rational value of  $u$ . It turns out that when  $u = 7/9$ , it becomes  $(32/3)^2$ . Using this solution, we can parametrize the fiber at  $t = 0$ :

$$u = \frac{7r^2 + 12r + 9}{9r^2 - 12r + 7}, \quad \delta = \frac{32(7r^2 + 12r + 9)(3r^2 + r - 3)}{(9r^2 - 12r + 7)^2},$$



where  $r$  is the parameter. This means that the cubic equation  $u^2 + xu + u = x^3$  in  $x$  with  $u$  given by the above formula is a cyclic polynomial. Let  $\xi_r$  be a root of the cubic polynomial

$$F_r(Z) = Z^3 - 4(7r^2 + 12r + 9)(9r^2 - 12r + 7)Z - 16(r^2 + 1)(7r^2 + 12r + 9)(9r^2 - 12r + 7).$$

Then,  $K_r = \mathbb{Q}(\xi_r, r)$  is a cyclic cubic extension of the field  $\mathbb{Q}(r)$ , and the point

$$P_r = (\xi_r, u) = \left( \xi_r, \frac{7r^2 + 12r + 9}{9r^2 - 12r + 7} \right)$$

belongs to  $E(K_r)$ . A straightforward height calculation shows that  $P_r$  is a point of infinite order.

Let  $a, b$  be relatively prime integers. By Silverman's result ([Sil]) the specializations of  $P_r$  to  $r = a/b$  have also infinite order except maybe for finitely many exceptions.

The discriminant of  $K_r/\mathbb{Q}(r)$  is

$$2^{10}(7r^2 + 12r + 9)^2(9r^2 - 12r + 7)^2(3r^2 + r - 3)^2.$$

Let  $K_{a/b}$  be the specialization of  $K_r$  with  $r = a/b$ . Then,  $K_{a/b}$  has square discriminant dividing

$$2^{10}(7a^2 + 12a + 9b^2)^2(9a^2 - 12ab + 7b^2)^2(3a^2 + ab - 3b^2)^2.$$

and the conductor of  $K_{a/b}$  is the square root of its discriminant. We let

$$H_1 = 7a^2 + 12a + 9b^2, \quad H_2 = 9a^2 - 12ab + 7b^2, \quad G = a^2 + b^2.$$

We note that the resultants of any pair of  $H_1, H_2$  and  $G$  is supported only at the primes 2, 3 and 37. Hence, if  $p$  is a rational prime  $p \neq 2, 3$  or 37, which divides  $H_1 H_2$  to the first power, then  $b^6 F_{a/b}(Z)$  is an Eisenstein polynomial at  $p$ , and therefore  $p$  ramifies (totally) in  $K_{a/b}/\mathbb{Q}$ .

On the other hand, if  $p$  divides  $3a^2 + ab - 3b^2$ , then we have

$$H_1 H_2 - 27G^2 = 4(3a^2 + ab - 3b^2) \equiv 0 \pmod{p},$$

and thus

$$b^6 F_{a/b}(Z) \equiv Z^3 - 108G^2Z - 432G^3 \equiv (Z + 6G)^2(Z - 12G) \pmod{p}.$$

It follows that the completion of  $K_{a/b}$  at the prime over  $p$  which contains  $Z - 12G$  is  $\mathbb{Q}_p$  and hence  $p$  splits completely in  $K_{a/b}$ .

Therefore we see that the conductor of  $K_{a/b}$  divides  $2^{10}H_1H_2$ . But  $H_1H_2$  is a separable binary form of degree 4 which is primitive. It follows from Stewart-Top ([ST, Theorem 1]) that the number of squarefree values less than  $X$  of  $H_1H_2$  is  $\gg X^{1/2}$ . We note that distinct squarefree values of  $H_1H_2$  yield distinct fields  $K_{a/b}$ . Therefore we have proved:

**Theorem 7.1.** *For the elliptic curve  $E37B$ , the number of cubic Dirichlet characters  $\chi$  for which  $L(E37B, 1, \chi) = 0$  satisfies*

$$\mathfrak{F}_E(3, X) = \#\{\chi \in \mathcal{X}(3) \mid \mathfrak{f}_\chi < X, L(E37B, 1, \chi) = 0\} \gg X^{1/2}.$$

We note that the calculations done above for the curve  $E37B$  actually work for any elliptic curve  $E/\mathbb{Q}$  with a  $\mathbb{Q}$ -rational point  $P$  of order 3 and which satisfies the condition below. We send the point  $P$  to  $(0, 0)$  and express  $E$  in the form

$$y^2 + 3Uxy + Ty = x^3.$$

where  $U, T \in \mathbb{Q}$ . The fibre over  $t = 0$ , on the surface  $\overline{S}_E$  takes the form

$$\delta^2 = -27u^2(u^2 - (4U^3 - 2T)u + T^2).$$

This may be expressed as a conic in the variables  $z = \delta/3u$  and  $w = u + 2U^3 - T$

$$z^2 + 3w^2 = 12U^3(U^3 - T).$$

This is a curve of genus zero and may be parameterized over  $\mathbb{Q}$  if a single rational point can be found. This occurs if and only if the right hand side is a norm from  $\mathbb{Q}(\sqrt{-3})$ , i.e., if and only if  $U(U^3 - T)$  is a norm from  $\mathbb{Q}(\sqrt{-3})$ .

These curves give examples for which  $\mathfrak{F}_E(3, X) \gg X^{1/2}$  mentioned in the introduction.

## REFERENCES

- [Akb] Amir Akbary, *Non-vanishing of weight  $k$  modular  $L$ -functions with large level*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 37–54.
- [Ant] *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Birch, B. J. and Kuyk, W. ed., Springer-Verlag, Berlin, 1975.
- [BCDT] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).
- [Ber] J. Bertin, *Réseaux de Kummer et surfaces de  $K3$* , Invent. Math. **93** (1988), 267–284.

- [BFH] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for  $L$ -functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618.
- [Chi] Gautam Chinta, *Nonvanishing twists of  $GL(2)$   $L$ -functions*, preprint, 11 pages.
- [Con] I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra **145** (1992), 463–467.
- [CKRS] B. Conrey, J. Keating, M. Rubinstein and N. Snaith, *On the frequency of vanishing of quadratic twists of modular  $L$ -functions*, Number theory for the Millenium I, A. K. Peters Ltd., Natick, (2002), pp. 301–315.
- [Cre] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.
- [DFK1] Chantal David, Jack Fearnley, and Hershy Kisilevsky, *On the vanishing of twisted  $L$ -functions of elliptic curves*, Experiment. Math. **13** (2004), no. 2, 185–198.
- [DFK2] C. David, J. Fearnley and H. Kisilevsky, *Vanishing of  $L$ -functions of elliptic curves over number fields*, Ranks of Elliptic Curves and Random Matrix Theory, London Mathematical Society Lecture Note Series, **341**, Cambridge University Press (2007), pp. 247–259.
- [Fea] Jack Fearnley, *Vanishing and non-vanishing of  $l$ -series of elliptic curves twisted by dirichlet characters*, Ph.D. thesis, Concordia University, 2001.
- [GM] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
- [Gol] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118.
- [Kato] K. Kato  *$p$ -adic Hodge theory and values of zeta functions of modular forms* Cohomologies  $p$ -adiques et applications arithmétiques. III, Astérisque **295** (2004), 117–290.
- [Kat] T. Katsura, *Generalized Kummer surfaces and their unirationality in characteristic  $p$* , J. Fac. Sci., Univ. Tokyo, Sect. I A **34** (1987), 1–41.
- [Kol] V. A. Kolyvagin, *Finiteness of  $E(\mathbf{Q})$  and  $SH(E, \mathbf{Q})$  for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.
- [KS] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.
- [Knapp] Anthony W. Knapp, *Elliptic curves*, Princeton University Press, 1992.
- [Kuw] M. Kuwata, *Canonical height and elliptic  $K3$  surfaces*, J. Number Theory **36** (1990), 399–406.
- [Mai] Liem Mai, *The average analytic rank of a family of elliptic curves*, J. Number Theory **45** (1993), no. 1, 45–60.
- [Mer] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math **124** (1996), 437–449.
- [MM] M. Ram Murty and V. Kumar Murty, *Mean values of derivatives of modular  $L$ -series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475.

- [MTT] B. Mazur, J. Tate, and J. Teitelbaum, *On  $p$ -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.
- [Mum] D. Mumford, *Abelian varieties*, Oxford University Press, 1970.
- [Mur] M. Ram Murty, *On simple zeros of certain  $L$ -series*, Number theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, pp. 427–439.
- [OS] K. Oguiso and T. Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, Comment. Math. Univ. Sancti Pauli **40** (1991), 83–99.
- [OS] Ken Ono and Christopher Skinner, *Fourier coefficients of half-integral weight modular forms modulo  $l$* , Ann. of Math. (2) **147** (1998), no. 2, 453–470.
- [Roh] David E. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, Automorphic forms and analytic number theory (Montreal, PQ, 1989), Univ. Montréal, Montreal, QC, 1990, pp. 123–133.
- [Roh2] ———, *Nonvanishing of  $L$ -functions and structure of Mordell-Weil groups*, J. Reine Angew. Math. **417** (1991), 1–26.
- [RS] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod  $p$  representations*, Conference on Elliptic Curves and Modular Forms, Hong Kong, December 18–21, 1993, Intl. Press, 1995, pp. 148–161.
- [Sch] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 379–460.
- [Ser] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
- [Shi] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.
- [Sil] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–251.
- [Sil] ———, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, New York, 1986.
- [ST] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), no. 4, 943–973.
- [Ste] Tomasz Stefanicki, *Non-vanishing of  $L$ -functions attached to automorphic representations of  $GL(2)$  over  $\mathbf{Q}$* , J. Reine Angew. Math. **474** (1996), 1–24.
- [TW] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.
- [Wal] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions  $L$  automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242.

(J. Fearnley) DEPARTMENT OF MATHEMATICS AND STATISTICS AND CICMA, CONCORDIA UNIVERSITY, 1455 DE MAISONNEUVE BLVD. WEST, MONTRÉAL, QUEBEC, H3G 1M8, CANADA

*E-mail address:* jack@mathstat.concordia.ca

(H. Kisilevsky) DEPARTMENT OF MATHEMATICS AND STATISTICS AND CICMA, CONCORDIA UNIVERSITY, 1455 DE MAISONNEUVE BLVD. WEST, MONTRÉAL, QUEBEC, H3G 1M8, CANADA

*E-mail address:* kisilev@mathstat.concordia.ca

(M. Kuwata) FACULTY OF ECONOMICS, CHUO UNIVERSITY, HACHIOJI-SHI, TOKYO 192-0393, JAPAN

*E-mail address:* kuwata@tamacc.chuo-u.ac.jp